适用于思科 AnyConnect 安全移动客户端的 Android 用户指南，版本 4.0.x

Revised: October 25, 2017,

AnyConnect 用户指南

安装和启动 AnyConnect

AnyConnect 概述

思科 AnyConnect 安全移动客户端 Android 版可提供安全无缝的企业网络远程访问。通过 AnyConnect，安装的应用可如同直接连接到企业网络一般进行通信。AnyConnect 是一款高级网络应用，可使您按照管理员的建议设置首选项、控制 AnyConnect 的操作，以及使用设备上的诊断工具和程序。

AnyConnect 可在您的企业中与移动设备管理软件配合使用。在这种情况下，请与管理员合作，确保遵守设备管理规则因为这些规则可能包括对一些已核准应用的 VPN 访问限制。您的组织可能会提供有关使用 AnyConnect Android 版的其他文档。

您的 Android 应用商店提供用于初始安装和所有升级的应用。思科自适应安全设备 (ASA) 是授权访问 VPN 的安全网关，但不支持 AnyConnect 适用于移动设备的更新。

开放式软件许可证说明

- 此产品包括 OpenSSL Project 开发的、可在 OpenSSL Toolkit 中使用的软件 (http://www.openssl.org/)。
- 此产品包括 Eric Young (eay@cryptsoft.com) 编写的加密软件。
- 此产品包括 Tim Hudson (tjh@cryptsoft.com) 编写的软件。

支持 Android 的设备

运行 Android 4.0 (Ice Cream Sandwich) 到最新版本 Android 7.0 (Nougat) 的设备上完全支持 Android 版思科 AnyConnect。

对于 Kindle Fire HD 设备和新版 Kindle Fire，可从 Amazon 获取 Kindle 版 Cisco AnyConnect。Kindle 版 AnyConnect 的功能与 Android 版 AnyConnect 软件包相当。

受管环境和非受管环境均支持每 Per App VPN。在使用 Samsung KNOX MDM 的受管环境下，需要有配备 Samsung Knox 2.0 的 Samsung 设备（运行 Android 4.3 或更高版本）。在非受管环境下使用 Per App 时，使用通用的 Android 方法。

对于网络可见性模块 (NVM) 功能，需要有运行 Samsung Knox 2.8 或更高版本的 Samsung 设备（需要 Android 7.0 或更高版本）。对于 NVM 配置，还需要 AnyConnect 4.4.3 或更高版本中的 AnyConnect 配置文件编辑器。早期版本不支持移动 NVM 配置。

有关安装和升级操作程序，请参阅 思科 AnyConnect 安全移动客户端用户指南，版本 4.0 (Android)。

安装 Android AnyConnect 应用

Android 版 AnyConnect 可从您的 Android 设备的 Android 市场下载，对于 Kindle 设备也可以从 Amazon 下载。不能从思科网站下载，也不能在连接到安全网关后下载。

若要安装 Android 版 AnyConnect，请按照正常程序下载、安装或升级设备上的应用。

启动 AnyConnect

过程

步骤 1 轻触 AnyConnect 图标启动 AnyConnect 应用。

步骤 2 如果这是在安装或升级 AnyConnect 后第一次启动，您会看到以下信息：

- 终端用户许可协议 (EULA)，您必须**接受**此协议才能继续。
- 针对数据收集的可接受的使用政策 (AUP)（如果网络管理员已配置了此项）。点击 **OK** 继续操作。数据收集由网络可见性模块 (NVM) 进行，该模块是 AnyConnect 客户端应用的一部分。

步骤 3 依次轻触**连接** > **添加新 VPN 连接**可配置连接条目。有关详细信息，请参阅手动添加连接条目，第 5 页。

步骤 4 （可选） 轻触 **Details**（**详细信息**）以查看当前活动 VPN 连接的摘要和详细统计数据。请参阅查看 AnyConnect 统计数据。

步骤 5 （可选） 轻触 **Menu**（**菜单**）并选择：

- **Settings**（**设置**），指定 AnyConnect 应用首选项。请参阅指定应用设置。
- **Diagnostics**（**诊断**），执行以下诊断活动：

  管理证书；请参阅关于 Android设备上的证书。

  管理 AnyConnect 配置文件；请参阅关于 AnyConnect 客户端配置文件。

  管理 AnyConnect 本地化；请参阅管理本地化。

  查看记录和系统信息；请参阅查看日志消息。

- **About**（**关于**），查看 AnyConnect 版本和许可证信息。请参阅显示 AnyConnect 版本和许可证。
- **Exit**（**退出**），退出 AnyConnect。请参阅退出 AnyConnect。

接下来的操作

按照管理员提供的说明配置和建立与网络的 VPN 连接。

Android 设备权限

适用于 AnyConnect 操作的 Android 清单中声明了以下权限：

清单权限	说明
uses-permission: android.permission.ACCESS_NETWORK_STATE	允许应用访问网络的相关信息。
uses-permission: android.permission.ACCESS_WIFI_STATE	允许应用访问 Wi-Fi 网络的相关信息。
uses-permission: android.permission.BROADCAST_STICKY	允许应用广播粘性意图。这些广播在完成后，其数据由系统保留，以便客户端可以快速检索这些数据，而不必等待下一次广播。
uses-permission: android.permission.INTERNET	允许应用打开网络套接字。
uses-permission: android.permission.READ_EXTERNAL_STORAGE	允许应用从外部存储中读取。
uses-permission: android.permission.READ_LOGS	允许应用读取低层系统日志文件。
uses-permission: android.permission.READ_PHONE_STATE	允许只读访问电话状态，包括设备的电话号码、当前的蜂窝网络信息、正在进行的任何呼叫的状态，设备上注册的任何电话帐户列表。
uses-permission: android.permission.RECEIVE_BOOT_COMPLETED	允许应用在系统完成启动后接收广播。

配置 VPN 连接

AnyConnect 需要以下信息以建立 VPN 连接：

- 用于访问您的网络的安全网关的地址。

  此地址在连接条目中配置。连接条目列在 AnyConnect 主屏幕上。活动的连接条目会在 AnyConnect 主屏幕上或连接列表中标识出来。VPN 连接条目可在设备上手动配置，或由企业管理员自动配置。

- 用于成功完成连接的身份验证信息。

  该信息的形式为您必须牢记的用户名和密码，或者包含在已在您的设备上配置的数字证书中。某些 VPN 连接可能同时需要这两种身份验证方法。数字证书可在设备上手动配置，或由设备管理员自动配置。

请按照管理员的指示配置您的 AnyConnect 客户端。如果您没有获得明确的说明，请与管理员联系。

配置连接条目

连接条目指定安全网关，该安全网关提供您的专用网络的访问权限以及其他连接属性。

在 AnyConnect 主屏幕中选择**连接**，以查看您的设备上已配置的条目。此处可能会列出多个连接条目。连接条目可能具有以下状态：

- 活动 - 此连接即当前处于活动状态的连接，会被标记或高亮显示。
- 已连接 - 此连接条目处于活动状态，当前已连接并正在运行。
- 已断开连接 - 此连接条目处于活动状态，但目前已断开连接，没有运行。

过程

连接条目可在设备上手动配置，或按以下方式自动配置：

- 手动配置。

  您必须知道网络的安全网关的地址。该地址是安全网关的域名或 IP 地址，它还可以指定您所属的组。还可以配置其他连接属性。请参阅手动添加连接条目，第 5 页。

- 通过点击管理员提供的链接自动配置。

  AnyConnect URI 链接可能包括在邮件中或发布在网页上。应用首选项 **External Control**（**外部控制**）必须设置为 **Prompt**（**提示**）或 **Enable**（**启用**），才能在您的设备上使用此功能。请参阅控制 AnyConnect 的外部使用，第 14 页

- 在连接到下载了包含连接条目的 AnyConnect 客户端配置文件的安全网关后进行自动配置。请参阅管理 AnyConnect 客户端配置文件，第 17 页。

- 通过您企业的移动设备管理软件进行配置。可在您的设备的 General Settings（常规设置）下找到设备管理配置文件。

手动添加连接条目

添加 VPN 连接条目以标识您要连接的 VPN 安全网关。

过程

步骤 1 在 AnyConnect 主窗口中，轻触 **Connection**（**连接**）> **Add New VPN Connection**（**添加新 VPN 连接**）以打开连接编辑器。
可随时**取消**连接编辑器。

步骤 2 （可选） 选择 **Description**（**说明**）以输入连接条目的描述性名称。
输入此连接条目的唯一名称。如果未指定，则使用 **Server Address**（**服务器地址**）作为默认名称。使用键盘显示上的任意字母、空格、数字或符号。此字段区分大小写。

步骤 3 选择 **Server Address**（**服务器地址**）以输入安全网关的地址。
输入安全网关的域名或 IP 地址，包括管理员指定的组（如果指定）。

步骤 4 （可选） 轻触 **Advanced Preferences**（**高级首选项**）以更改高级证书和协议设置。
可随时**取消** Advanced Connection Editor（高级连接编辑器）窗口。

步骤 5 （可选） 轻触 **Certificate**（**证书**）以指定此连接如何使用用户证书。

- 轻触 **Disabled**（**禁用**）将指定此连接不使用证书。
- 轻触 **Automatic**（**自动**）将指定仅当安全网关要求时才使用证书建立连接。
- 轻触管理员指示您使用的证书。

如果建立VPN会话需要用户证书，管理员将为您提供在移动设备上安装用户证书的说明。轻触列表中的任意证书可查看其详细信息。

步骤 6 （可选） 轻触 **Connect with IPsec**（**使用 IPsec 连接**）以对此 VPN 连接使用 IPsec 而不是 SSL。
此连接属性由管理员为您提供。

如果选择的 VPN 连接协议为 IPsec，则 **Authentication**（**身份验证**）参数变为活动状态。

步骤 7 （可选） 轻触 **Authentication**（**身份验证**）并选择该 IPsec 连接的身份验证方法。
此连接属性由管理员为您提供。

- EAP-AnyConnect（默认身份验证选项）
- IKE-RSA
- EAP-GTC
- EAP-MD5
- EAP-MSCHAPv2

您的身份验证选项显示在 **Advanced Connection Editor**（**高级连接编辑器**）窗口中。

步骤 8 （可选） 如果已指定使用 EAP-GTC、EAP-MD5 或 EAP-MSCHAPv2 进行身份验证，则轻触 **IKE Identity**（**IKE 标识**）输入管理员提供的标识信息。

步骤 9 轻触 **Advanced**（**高级**）窗口和 **Connection Editor**（**连接编辑器**）窗口中的 **Done**（**完成**）以保存连接值。
AnyConnect 即添加新连接条目。

修改连接条目

更改 VPN 连接条目以纠正配置错误或符合 IT 策略更改。

注释 您无法修改从安全网关下载的连接条目的描述或服务器地址。

过程

步骤 1 在 AnyConnect 主窗口中，轻触**连接**。然后，长按连接条目以显示**选择操作**窗口。

步骤 2 轻触 **Edit connection**（**编辑连接**）。

Connection Editor（**连接编辑器**）窗口显示分配到连接条目的参数值。

步骤 3 轻触要修改的值，使用屏幕键盘输入新值，然后轻触 **OK**（**确定**）。

步骤 4 轻触 **Done**（**完成**）。
AnyConnect 将保存已修改的连接条目。

删除连接条目

此过程可删除手动配置的 VPN 连接条目。删除从 VPN 安全网关导入的连接条目的唯一方法是删除下载的包含连接条目的 AnyConnect 配置文件。

过程

步骤 1 在 AnyConnect 主窗口中，轻触**连接**。然后，长按连接条目以显示**选择操作**窗口。

步骤 2 依次轻触**删除连接**。

配置证书

关于 Android设备上的证书

证书可以数字方式标识 VPN 连接的两端：安全网关或服务器，以及 AnyConnect 客户端或用户。服务器证书可标识 AnyConnect 的安全网关，用户证书可标识安全网关的 AnyConnect 用户。证书从证书颁发机构 (CA) 获取并由其验证。

当建立连接时，AnyConnect 始终期待从安全网关获得服务器证书。安全网关只有在经过相应配置后才会期待从 AnyConnect 获得证书。期待 AnyConnect 用户手动输入凭证是对 VPN 连接进行身份验证的另一种方式。事实上，安全网关可以配置为通过数字证书、手动输入凭证或同时采用这两种方式对 AnyConnect 用户进行身份验证。仅使用证书的身份验证允许 VPN 在不需要用户干预的情况下进行连接。

请按照管理员的指示，将证书分配到安全网关和设备，以及在安全网关和设备中使用证书。同时，按照管理员的指示导入、使用和管理 AnyConnect VPN 的服务器证书和用户证书。本文档提供了与证书和证书管理有关的信息和过程，以便您了解和参考。

AnyConnect 将用于身份验证的用户证书和服务器证书存储在 Android 设备上的 AnyConnect 证书存储区中。通过 **Menu**（**菜单**）> **Diagnostics**（**诊断**）> **Certificate Management**（**证书管理**）屏幕可管理 AnyConnect 证书存储区；您也可以在此处查看 Android 系统证书。

关于用户证书
为了让 AnyConnect 用户使用数字证书进行安全网关的身份验证，您的设备上的 AnyConnect 证书存储区中需要有一个用户证书。按照管理员的指示，使用以下方法之一导入用户证书：

- 点击管理员通过电邮或在网页上提供的超链接后自动导入。
- 手动从设备的文件系统、设备的凭证存储或网络服务器导入。

- 在连接到由管理员配置为提供证书的安全网关时导入。

导入后，可以将证书与特定连接条目关联，或者在建立连接进行身份验证期间自动选择证书。

如果不再需要 AnyConnect 存储区中的用户证书进行身份验证，可以将它们删除。

关于服务器证书
当且仅当在连接建立期间从安全网关接收的服务器证书有效且受信任时，该证书才会自动向 AnyConnect 验证服务器的身份。其他:

- 有效但不受信任的服务器证书可以被审核、授权和导入到AnyConnect证书存储区中。当服务器证书导入到AnyConnect存储区后，后续的使用该数字证书建立的与服务器的连接会被自动接受。
- 无效证书无法导入到 AnyConnect 存储区中。可以接受该证书以完成当前连接，但不推荐这样做。

如果不再需要 AnyConnect 存储区中的服务器证书进行身份验证，可以将它们删除。

从超链接导入证书

管理员将为您提供用于在您的设备上安装证书的超链接。

开始之前

在 AnyConnect 设置中将 **External Control**（外部控制）设置为 **Prompt**（提示）或 **Enable**（启用）。

过程

步骤 1 轻触管理员提供的超链接。

链接可包含在电邮中，也可发布在内联网网页上。

步骤 2 如果出现提示，则输入提供给您的证书的身份验证代码。

证书安装在 Android 设备上的 AnyConnect 证书存储区中，可以被查看、分配到连接条目或删除。

手动导入证书

以下内容说明了为进行 VPN 身份验证而手动将用户证书导入到 AnyConnect 存储区的所有可能选项。

开始之前

从管理员处获取具体的证书导入过程。

过程

步骤 1 在 AnyConnect 主窗口中，轻触 **Menu**（菜单）> **Diagnostics**（诊断）> **Certificate Management**（证书管理）。

步骤 2 轻触 **User**（用户）选项卡。

步骤 3 轻触 **Import**（导入）以导入证书。

步骤 4 选择导入源：

- 轻触 **File System**（文件系统）可从本地文件系统导入证书文件。
- 轻触 **Network Location (URI)**（网络位置 (URI)）可从网络上的服务器导入证书。
- 轻触 **Device Credential Storage**（设备凭证存储）可链接到当前位于设备凭证存储中的证书。

  源证书实际上不会复制到 AnyConnect 证书存储区中。如果从凭证存储中删除证书，该证书的链接也会同时删除。

  注释
  - 此选项仅适用于运行 Android 4.0 (Ice Cream Sandwich) 或更高版本的设备。
  - 在 Android 4.1 (Jelly Bean) 上尝试从设备凭证存储区导入证书时，客户端将显示错误消息“此 Android 版本不支持此功能。”将证书直接导入到 AnyConnect 存储区，而不使用 Android 本机存储区。

导入安全网关提供的证书

开始之前

管理员将安全网关配置为启用证书分配并提供该安全网关的连接信息。

过程

步骤 1 打开 AnyConnect。

步骤 2 在 **Choose a connection**（选择连接）区域中，轻触能将证书下载到您的移动设备的连接的名称。

步骤 3 如果存在，轻触 **Get Certificate**（获取证书），或选择已配置为将证书下载到您的移动设备的组。

步骤 4 输入管理员提供的身份验证信息。

安全网关将证书下载到您的设备。您的 VPN 会话断开，您收到证书注册成功的消息。

查看证书

查看已导入到 AnyConnect 证书存储区中的用户证书和服务器证书，以及 Android 系统证书。

过程

步骤 1 在 AnyConnect 主窗口中，轻触 **Menu**（菜单）> **Diagnostics**（诊断）> **Certificate Management**（证书管理）。

步骤 2 轻触 **User**（用户）或 **Server**（服务器）选项卡以查看 AnyConnect 证书存储区中的证书。

长按证书并轻触：

- **View certificate details**（查看证书详细信息）可查看证书的内容。
- **Delete certificate**（删除证书）可从 AnyConnect 存储区中删除此证书。

步骤 3 轻触 **System**（系统）选项卡可查看 Android 凭证存储中的证书。

长按证书并轻触 **View certificate details**（查看证书详细信息）可查看证书的内容。

删除证书

只能删除 AnyConnect 证书存储区中的证书；不能删除系统证书存储区中的证书。

可以从 AnyConnect 证书存储区单独删除证书，也可以一次全部清除。

删除单个证书

过程

步骤 1 在 AnyConnect 主窗口中，轻触 **Menu**（菜单）> **Diagnostics**（诊断）> **Certificate Management**（证书管理）。

步骤 2 轻触 **User**（用户）或 **Server**（服务器）选项卡以显示 AnyConnect 证书存储区中的用户证书或服务器证书。

步骤 3 长按证书。

将显示 **Certificate Options**（证书选项）。

步骤 4 选择 **Delete certificate**（删除证书）并确认您要删除该特定证书。

清除所有证书

过程

步骤 1 在 AnyConnect 主窗口中，轻触 **Menu**（菜单）> **Diagnostics**（诊断）> **Certificate Management**（证书管理）。

步骤 2 轻触 **User**（用户）或 **Server**（服务器）选项卡以显示 AnyConnect 证书存储区中的用户证书或服务器证书。

步骤 3 轻触 **Clear All**（全部清除）以删除 AnyConnect 证书存储区中的所有证书。

建立 VPN 连接

通过轻触与 **AnyConnect VPN** 面板中显示的活动连接相关联的复选框或滑块，或者选择 AnyConnect 主屏幕中列出的其他连接条目之一来连接到 VPN。

开始之前

- 您必须有活动的 Wi-Fi 连接或已经与服务提供商连接才能连接到 VPN。
- 要发起 VPN 连接，您必须至少有一个连接条目在 AnyConnect 主窗口上的 **Choose a Connection**（**选择连接**）下列出。
- 要完成 VPN 连接，您必须有安全网关所需的身份验证信息。

过程

步骤 1 转到 AnyConnect 主窗口。

步骤 2 轻触**连接**，然后轻触要使用的连接条目。

AnyConnect 发起 VPN 连接时，会断开当前正在使用的任何 VPN 连接，并使所选连接条目成为当前连接。

步骤 3 如有必要，请执行以下操作之一以响应身份验证提示：

- 输入您的用户名和密码凭证。如果管理员配置了双重身份验证，系统可能还会提示您输入二级凭证。
- 轻触 **Get Certificate**（**获取证书**）并输入管理员提供的证书注册凭证。AnyConnect 会保存证书并重新连接到 VPN 安全网关以使用该证书进行身份验证。

根据 VPN 安全网关配置，AnyConnect 可能会向 AnyConnect 主窗口中的列表添加连接条目。AnyConnect 主窗口的顶行会突出显示复选标记，指示 VPN 连接已建立。

注释 轻触 AnyConnect 主窗口中的其他 VPN 连接会断开当前 VPN 连接，并连接到与您轻触的 VPN 连接相关联的 VPN 安全网关。

响应 AnyConnect 通知

响应不受信任的 VPN 服务器通知

所显示的**不受信任的 VPN 服务器**通知的类型取决于 **Block Untrusted VPN Server**（**阻止不受信任的 VPN 服务器**）应用首选项：

- 如果已启用，则显示阻止**不受信任的 VPN 服务器！**通知，请选择：
  - **Keep Me Safe**（**保证我的安全**）可保持此设置以及此阻止行为。

- **Change Settings**（**更改设置**）可取消阻止。

  在更改 **Block Untrusted VPN Server**（**阻止不受信任的 VPN 服务器**）后，重新发起 VPN 连接。

- 如果未启用，则显示未阻止**不受信任的 VPN 服务器**！通知，请选择：

  Cancel（**取消**）可中止与不受信任服务器的 VPN 连接。

  Continue（**继续**）可与不受信任的服务器建立连接；不推荐使用此选项。

  View Details（**查看详细信息**）可查看证书详细信息并决定是否将服务器证书导入到 AnyConnect 证书存储区中以备将来接受，同时继续连接。

响应其他应用

为保护您的设备，当外部应用试图使用 AnyConnect 时，AnyConnect 将提醒您。当 AnyConnect 应用首选项 **External Control**（**外部控制**）设置为 **Prompt**（**提示**）时，会发生这种情况。

对于以下提示，请询问管理员是否轻触 **Yes**（**是**）来响应：

- `Another application has requested that AnyConnect create a new connection to host.（其他应用请求 AnyConnect 创建到主机的新连接。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]`
- `Another application has requested that AnyConnect connect to host.（其他应用请求 AnyConnect 连接到主机。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]`
- `Another application has requested that AnyConnect disconnect the current connection.（其他应用请求 AnyConnect 断开当前连接。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]`
- `Another application has requested that AnyConnect import a certificate bundle to the AnyConnect certificate store.（其他应用请求 AnyConnect 将一个证书捆绑包导入到 AnyConnect 证书存储区。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]`
- `Another application has requested that AnyConnect import localization files.（其他应用请求 AnyConnect 导入本地化文件。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]`
- `Another application has requested that AnyConnect import profiles.（其他应用请求 AnyConnect 导入配置文件。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]`

响应 MMS 通知

连接 AnyConnect VPN 后，您无法检索或发送多媒体 (MMS) 消息。如果尝试后被阻止，状态栏中将显示一个 MMS 通知图标。要确认此通知：

过程

步骤 1　轻触通知图标可查看通知。

步骤 2　轻触通知可查看服务影响。

步骤 3　如果您不想再接收 MMS 通知，请选中 **Do not show this again**（**不再显示此通知**）复选框。

注意　这是永久选项。您将来无法撤消此操作。

步骤 4　点击 **OK**（**确定**）。

可选 AnyConnect 配置和管理

指定应用设置

启动时启动 AnyConnect

您可以控制何时在您的设备上启动 AnyConnect。默认情况下，AnyConnect 不会在设备启动时自动启动。如果选中，则启用“Launch at Startup（启动时启动）”。

注释　如果下载或导入了指定“值得信赖的网络检测”的配置文件，则自动启用“Launch at Startup（启动时启动）”。

过程

步骤 1　在 AnyConnect 主窗口中，依次轻触**菜单** > **设置**。

步骤 2　轻触 **Launch at Startup**（**启动时启动**）复选框可启用或禁用此首选项。

隐藏 AnyConnect 状态栏图标

当 AnyConnect 处于非活动状态时，可以隐藏通知栏中的 AnyConnect 图标。

过程

步骤 1　在 AnyConnect 主窗口中，依次轻触**菜单** > **设置**。

步骤 2　轻触 **Hide Icon**（**隐藏图标**）复选框。

如果保持未选中状态，图标将持续显示。

控制 AnyConnect 的外部使用

External Control（外部控制）应用设置指定 AnyConnect 应用如何响应外部 URI 请求。外部请求创建连接条目；连接或断开 VPN；导入客户端配置文件、证书或本地化文件。

外部请求通常由管理员通过电邮或在网页上提供。管理员将指示您使用以下值之一：

- Enabled（启用）- AnyConnect 应用自动允许所有 URI 命令。
- Disabled（禁用）- AnyConnect 应用自动禁止所有 URI 命令。
- Prompt（提示）- 每次在设备上访问 AnyConnect URI 时，AnyConnect 应用都会提示您。您可以允许或禁止 URI 请求。有关详细信息，请参阅 响应其他应用，第 12 页。

过程

步骤 1 在 AnyConnect 主窗口中，依次轻触**菜单** > **设置**。

步骤 2 轻触 **External Control**（外部控制）。

步骤 3 轻触 **Enabled**（启用）、**Disabled**（禁用）或 **Prompt**（提示）。

阻止不受信任的服务器

此应用设置确定当 AnyConnect 无法识别安全网关时是否阻止连接。默认情况下此保护处于打开状态；可以关闭此保护，但不推荐这样做。

AnyConnect 使用从服务器接收到的证书来验证其标识。如果存在由于过期或日期无效、密钥使用错误或名称不匹配而导致的证书错误，连接将被阻止。

当开启此设置时，阻止**不受信任的 VPN 服务器**！通知会提示您此安全威胁。

过程

步骤 1 在 AnyConnect 主窗口中，依次轻触**菜单** > **设置**。

步骤 2 轻触 **Block Untrusted Servers**（阻止不受信任的服务器）复选框以启用或禁用此首选项。

设置 FIPS 模式

在 FIPS 模式下，所有 VPN 连接均使用联邦信息处理标准 (FIPS) 加密算法。

开始之前

如果您需要在移动设备上启用 FIPS 模式才能连接到网络，管理员将通知您。

过程

步骤 1 在 AnyConnect 主窗口中，依次轻触**菜单** > **设置**。

步骤 2 轻触 **FIPS Mode**（**FIPS 模式**）以启用或禁用此首选项。

在确认 FIPS 模式更改后，AnyConnect 将退出，必须手动重新启动。重新启动后，FIPS 模式设置生效。

设置 OCSP 吊销

Android AnyConnect 客户端支持 OCSP（在线证书状态协议）。由此，使客户端可以实时查询各个证书的状态，具体方法为：向 OCSP 响应程序发送请求，并解析 OCSP 响应，即可获得证书状况。OCSP 用于验证整个证书链。对于每个证书，访问 OCSP 响应程序设有五秒的超时间隔。

开始之前

如果需要在移动设备上启用“OCSP 吊销”以便连接网络，管理员将会通知您。

过程

步骤 1 在 AnyConnect 主窗口中，依次轻触**菜单** > **设置**。

步骤 2 轻触 **OCSP 吊销**可启用或禁用此首选项。

在下一次尝试连接时，系统将使用（或不使用）OCSP 来确定从头端获得的证书的吊销状态。

严格证书信任

如果选择该选项，在对远程安全网关进行身份验证时，AnyConnect 将禁用没有用户干预则无法自动验证的所有证书。客户端会连接失败，而不是提示用户接受这些证书。此设置将覆盖“阻止不受信任的服务器”。

如果未选择该选项，客户端将提示用户接受或拒绝证书。此为默认行为。

开始之前

如果需要在移动设备上启用“严格证书信任”以便连接网络，管理员将会通知您。

过程

步骤 1 在 AnyConnect 主窗口中，依次轻触**菜单** > **设置**。

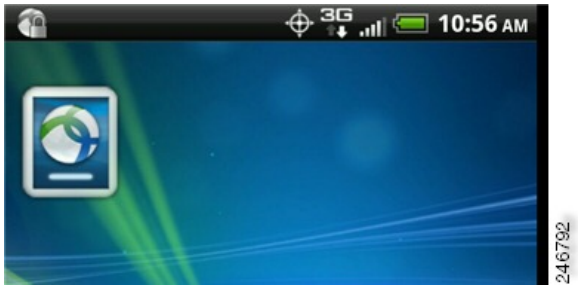
步骤 2 轻触**严格证书信任**可启用或禁用此首选项。

在下一次尝试连接时，系统将使用（或不使用）“严格证书信任”来确定用户是否可以选择接受从头端获取的未经验证的证书。

使用 AnyConnect 构件

AnyConnect 提供了可添加到主屏幕的构件：

- 最小的构件的大小与 AnyConnect 应用图标相同。图标下横条的颜色可反映 VPN 状态。轻触该构件可连接到 VPN 或断开当前 VPN 连接。



- 较大的构件显示 AnyConnect 图标和名称、当前 VPN 连接以及 VPN 状态。轻触该构件可连接到 VPN 或断开 VPN 连接。

放置构件的说明可能会因您使用的具体设备和 Android 版本而有所不同。下文介绍的是示例说明。

过程

步骤 1 转到有足够空间放置您要使用的构件的 Android 主屏幕。

步骤 2 轻触 **Menu**（菜单）> **Personalize**（个人化）> **Widgets**（构件）。

步骤 3 轻触要使用的 AnyConnect 构件。

Android 可将构件添加到主屏幕。

步骤 4 如果要重新放置构件，请长按构件。构件响应后，请移动构件。

管理 AnyConnect 客户端配置文件

关于 AnyConnect 客户端配置文件

AnyConnect VPN 客户端配置文件是一个 XML 文件，用于指定客户端行为和标识 VPN 连接。VPN 客户端配置文件中的每个连接条目都指定可访问此设备的安全网关以及其他连接属性、策略和限制。除了您在设备本地配置的 VPN 连接以外，这些连接条目均列在 AnyConnect 主屏幕上，在发起 VPN 连接时可进行选择。

AnyConnect 一次只在 Android 设备上保留一个 VPN 客户端配置文件。以下是导致当前配置文件（如果存在）被替换或删除的一些主要情景：

- 手动导入配置文件会将当前配置文件替换为导入的配置文件。
- 在自动或手动 VPN 连接启动时，新连接的配置文件将替换当前配置文件。
- 如果 VPN 连接没有配置文件与之关联，该 VPN 启动时将删除现有配置文件。

查看或删除设备上当前的 AnyConnect 配置文件，或导入新配置文件。

查看 AnyConnect 配置文件

过程

步骤 1 在 AnyConnect 主窗口中，轻触 **Menu**（菜单）> **Diagnostics**（诊断）> **Profile Management**（配置文件管理）。

步骤 2 轻触扩展图标以获取**当前配置文件详细信息**。将显示 XML 文件。向下滚动可查看整个文件。

导入 AnyConnect 配置文件

开始之前

配置文件必须位于 Android 设备中才能以这种方式导入。管理员提供要在您的设备上安装的配置文件的名称。

过程

步骤 1 在 AnyConnect 主窗口中，轻触 **Menu**（菜单）> **Diagnostics**（诊断）> **Profile Management**（配置文件管理）。

步骤 2 轻触 **Import Profile**（导入配置文件）并从设备的文件系统中选择 XML 配置文件。

此配置文件中定义的连接条目会立即显示在 AnyConnect 主屏幕中，并且 AnyConnect 客户端的行为将遵守此配置文件的规范。

删除 AnyConnect 配置文件

过程

步骤 1 在 AnyConnect 主窗口中，轻触 **Menu** > **Diagnostics** > **Profile Management**。

步骤 2 轻触 **Delete Profile** 并确认以删除当前配置文件。

配置文件中定义的连接条目将从 AnyConnect 主屏幕清除，并且 AnyConnect 客户端行为符合默认客户端规范。

管理本地化

查看已安装的本地化数据

安装 AnyConnect 时，如果设备的指定区域设置与某个打包的语言翻译匹配，则您的移动设备将被本地化。AnyConnect 软件包中包括以下语言翻译：

- 加拿大法语 (fr-ca)
- 中文（台湾地区）(zh-tw)
- 捷克语 (cs-cz)
- 荷兰语 (nl-nl)
- 法语 (fr-fr)
- 德语 (de-de)
- 匈牙利语 (hu-hu)
- 意大利语 (it-it)
- 日语 (ja-jp)
- 韩语 (ko-kr)

- 拉丁美洲西班牙语 (es-co)
- 波兰语 (pl-pl)
- 葡萄牙语（巴西）(pt-br)
- 俄语 (ru-ru)
- 简体中文 (zh-cn)
- 西班牙语 (es-es)

安装的语言取决于 **设置** > **语言和键盘** > **选择区域设置**中指定的区域设置。AnyConnect 启动后，AnyConnect 用户界面和消息会立即翻译为本地语言。

AnyConnect 会依次使用语言规范和地区规范来确定最佳匹配设置。例如，安装完成后，在法语-瑞士(fr-ch) 区域设置下，最终的显示为法语-加拿大(fr-ca)。

过程

步骤 1 在 AnyConnect 主窗口中，依次轻触**菜单** > **诊断** > **本地化管理**。

步骤 2 查看您的移动设备上已安装的本地化文件列表。

指示的语言是 AnyConnect 当前正在使用的语言。

导入本地化数据

安装后，通过以下方式导入 AnyConnect 软件包不支持的语言的本地化数据：

- 点击管理员提供的已定义为导入本地化数据的超链接。

  管理员可以通过电邮或网页提供超链接，点击该超链接将导入本地化数据。此方法使用 AnyConnect URI 处理程序，这是为管理员提供的一个功能，用于简化 AnyConnect 配置和管理。

  注释 您必须在 AnyConnect 设置中将 External Control（外部控制）设置为 Prompt（提示）或 Enable（启用）以允许该 AnyConnect 活动。有关如何进行设置的信息，请参阅控制 AnyConnect 的外部使用 ， 第 14 页。

- 连接到已被管理员配置为通过 VPN 连接提供可下载的本地化数据的安全网关。

  如果要使用此方法，管理员会通过 XML 配置文件提供相应的 VPN 连接信息或预定义的连接条目。本地化数据可通过 VPN 连接下载到您的设备并立即生效。

- 使用“AnyConnect 本地化管理活动”屏幕上的**导入本地化**选项可手动导入，如以下所述。

过程

步骤 1 在 AnyConnect 主窗口中，依次轻触**菜单** > **诊断** > **本地化管理**。

步骤 2 轻触 **Import Localization**（**导入本地化**）。

步骤 3 指定安全网关的地址和区域设置。

根据 ISO 639-1 指定区域设置，如适用，可添加国家代码（例如，en-US、fr-CA、ar-IQ 等等）。

此本地化数据用来替代预先打包的已安装的本地化数据。

恢复本地化数据

过程

步骤 1 在 AnyConnect 主窗口中，依次轻触**菜单** > **诊断** > **本地化管理**。

步骤 2 轻触 **Restore Localization**（**恢复本地化**）。

恢复使用 AnyConnect 软件包中预装的本地化数据并删除所有已导入的本地化数据。

系统将根据**设置** > **语言和键盘** > **选择区域设置**中指定的设备区域设置选择恢复的语言。

退出 AnyConnect

退出 AnyConnect 将终止当前 VPN 连接并停止所有 AnyConnect 进程。请谨慎使用此操作。您的设备上的其他应用或进程可能正在使用当前 VPN 连接，退出 AnyConnect 可能会对其操作造成不利影响。

过程

在 AnyConnect 主窗口中，轻触 **Menu**（**菜单**） > **Exit**（**退出**）。

如果 AnyConnect 无法顺利退出其所有进程，您将转到 Android 应用管理屏幕，在此处可通过轻触 **Force Stop**（**强制停止**）来手动终止 AnyConnect。

删除 AnyConnect

过程

步骤 1 转到设备的 Android 设置并进入应用或应用管理区域。

步骤 2 轻触 **Uninstall**（卸载）。

对 AnyConnect 进行监控和故障排除

显示 AnyConnect 版本和许可证

过程

在 AnyConnect 主窗口中，轻触 **Menu**（菜单） > **About**（关于）。

接下来的操作

轻触 **About**（关于）窗口中的链接可打开本指南的最新版本。

确定连接状态

默认情况下，AnyConnect 通过更改其图标来显示其状态（该图标位于 Android 窗口顶部的 Android 状态栏中）。图标指示 AnyConnect 连接的当前状态：

查看 AnyConnect 统计数据

当存在 VPN 连接时，AnyConnect 会记录统计数据。

过程

在 AnyConnect 主屏幕中，轻触 **Details**（详细信息）。

详细统计数据包括以下值：

- 安全路由 - 目标为 0.0.0.0 和子网掩码为 0.0.0.0 的条目表示所有 VPN 流量均加密，并通过 VPN 连接发送或接收。
- 不安全路由 - 仅当 SecureRoutes.Traffic 目标下存在 0.0.0.0/0.0.0.0（由 VPN 安全网关确定，从加密连接中排除）时才显示。

AnyConnect 日志记录

查看日志消息

过程

步骤 1 在 AnyConnect 主窗口中，轻触 **Menu**（菜单）> **Diagnostics**（诊断）> **Logging and System Information**（记录和系统信息）。

AnyConnect 会检索其消息，并在 Messages（消息）、System（系统）和 Debug（调试）窗口中显示它们。

步骤 2 轻触 **Messages**（消息）、**System**（系统）或 **Debug**（调试）选项卡以查看日志消息或系统信息。

- Messages（消息）：与 AnyConnect 活动有关的日志。
- System（系统）：与内存、接口、路由、过滤器、权限、进程、系统属性、内存映射和唯一设备 ID 有关的信息。
- Debug（调试）：管理员和思科技术支持中心 (TAC) 用来分析 AnyConnect 问题的日志。

步骤 3 滚动窗口可查看所有消息。

发送日志消息

过程

步骤 1 在 AnyConnect 主窗口中，轻触 **Menu**（菜单）> **Diagnostics**（诊断）> **Logging and System Information**（记录和系统信息）。

步骤 2 依次轻触**菜单** > **发送日志**。

日志消息和所有配置文件数据将打包成一个 .zip 文件并插入到电邮消息中。如果要报告 AnyConnect 的问题，请使用电邮选项将日志文件发送给管理员。在发送日志消息前，必须详细说明问题和重现问题的步骤。

使用蓝牙进行本地传输。必须先在发送设备和接收设备上启用蓝牙。

清除调试日志消息

过程

步骤 1 在 AnyConnect 主窗口中，轻触 **Menu**（菜单） > **Diagnostics**（诊断） > **Logging and System Information**（记录和系统信息）。

步骤 2 依次轻触**菜单** > **清除调试日志**。

Android 常见问题

我收到了 tun.ko 错误消息

如果 tun.ko 模块尚未编译到内核中，则需要该模块。如果该模块没有包含在设备中，也没有与内核一起编译，请为相应的设备内核获取或编译该模块，然后将其放在 /data/local/kernel_modules/ 目录下。

我无法编辑/删除某些连接条目

管理员在 AnyConnect 配置文件中定义了这些连接条目。有关删除这些配置文件的说明，请参阅“查看和管理 AnyConnect 配置文件”。

连接超时和无法解析主机

互联网连接问题、蜂窝信号强度低以及网络资源拥塞是超时和无法解析主机错误的常见起因。尝试选择信号更强的区域或使用 WiFi。如果有可用的 Wi-Fi 网络，先尝试使用设备的“设置”应用与网络建立连接。对于超时问题，重试多次通常会连接成功。

基于证书的身份验证不可用

如果以前成功过，请检查证书的有效性和到期日期。要执行此操作，请转到 AnyConnect 主窗口，长按连接条目，然后轻触 **Certificate**（证书）。Certificates（证书）窗口此时将列出所有证书。长按证书名称，然后轻触 **View Certificate Details**（查看证书详细信息）。与管理员联系，以确保您使用合适的证书进行连接。

连接时出错，设备工作正常

询问管理员 VPN 安全网关是否已配置并已被授权允许移动连接。

无法连接到 ASA，无法解析主机错误

使用互联网浏览器检查网络连接。要验证网络连接，请转到 https://vpn.example.com，其中 vpn.example.com 是 VPN 安全网关的 URL。

从 Market 安装 AnyConnect 软件包失败。

确保设备已被列为支持的 Android 设备。

“Installation Error: Unknown reason -8”（安装错误：未知原因 -8）

如果您尝试在不受支持的设备上安装品牌特定的 AnyConnect 软件包，设备将收到此消息。查看支持的 Android 设备列表以及安装或升级 AnyConnect 的说明，以下载适合设备的 AnyConnect 软件包。

AnyConnect 错误，“Could not obtain the necessary permissions to run this application.This device does not support AnyConnect.”（无法获取运行此应用所需的权限。此设备不支持 AnyConnect。）

AnyConnect 在此设备上不工作。查看支持的 Android 设备列表以及安装或升级 AnyConnect 的说明，以下载适合设备的 AnyConnect 软件包。

由于网络连接问题，无法通过电邮发送日志

尝试其他可访问互联网的网络。如果没有网络连接或者您需要重置设备，请将日志消息保存在电邮消息草稿中。

AnyConnect 频繁自行连接

这可能是由值得信赖的网络检测/自动 VPN 策略引起的。在 AnyConnect 设置中禁用 TND 应用首选项将此功能关闭。

使用一次性密码的身份验证不可用

由于 Android 问题，当粘贴剪贴板中的文本时，系统会在文本前插入一个空格。在 AnyConnect 中，复制一次性密码之类的文本时，用户必须删除这个错误的空格。

Android 版 AnyConnect 的准则和限制

- Android 版 AnyConnect 仅支持与远程接入切实相关的 VPN 功能。
- Android 版 AnyConnect 仅支持网络可见性模块，不支持任何其他 AnyConnect 模块。
- ASA 不对 Android 版 AnyConnect 提供分发和更新。它们仅在 Google Play 中提供。
- Android 版 AnyConnect 支持用户添加的连接条目以及由 ASA 所推送的 AnyConnect 配置文件填入的连接条目。Android 设备仅支持一个 AnyConnect 配置文件，即，从头端接收的最后一个配置文件。但是，一个配置文件可能包含多个连接条目。
- 如果用户尝试在不受支持的设备上安装 AnyConnect，将收到弹出消息 `安装错误：原因未知 -8 (Installation Error: Unknown reason -8)`。此消息由 Android OS 生成。
- 如果用户在其主屏幕上安装 AnyConnect 构件，那么，无论是否选择了“在启动时启动”(Launch at startup) 首选项，AnyConnect 服务都将自动启动（但不连接）。
- 使用“从客户端证书预填充”功能时，Android 版 AnyConnect 需要对扩展的 ASCII 字符进行 UTF-8 字符编码。根据 KB-890772 和 KB-888180 中的说明，如果您想使用预填充，客户端证书必须采用 UTF-8 格式。
- AnyConnect 在通过 EDGE 连接发送或接收 VPN 流量时会阻止语音呼叫，这是 EDGE 和其他早期无线电技术的固有性质所决定的。

- 一些已知的文件压缩实用程序无法成功解压缩使用 AnyConnect“发送日志”(Send Log) 按钮打包的日志捆绑包。其解决方法是使用 Windows 和 Mac OS X 上的本地实用程序解压缩 AnyConnect 日志文件。

已知兼容性问题

- 公共接口和专用接口上的 IPv6。

  在 Android 5 及更高版本中，使用 AnyConnect 4.05015 及更高版本的专用传输和公共传输均支持 IPv6。对于此组合，目前允许以下配置：在 IPv6 隧道上传输 IPv4、在 IPv6 隧道上传输 IPv6。

  另外，还支持早期 AnyConnect 和 Android 版本中以前允许的隧道配置：在 IPv4 隧道上传输 IPv4 和在 IPv4 隧道上传输 IPv6。

  注释 由于 Google 问题 65572，通过 IPv4 传输 IPv6 在 Android 4.4 中不起作用。您必须使用 Android 5 或更高版本。

- 节电模式和 AnyConnect：

  Android 5.0 引入了节电模式功能，该功能会阻止设备上的后台网络连接。启用节电模式后，在后台运行的 AnyConnect 将转换为“已暂停”(Paused) 状态。若要解决 Android 5.0 上的这一问题，用户可以通过设备设置“设置”(Settings) -> “电池”(Battery) -> “节电模式”(Battery saver) 或从通知栏关闭节电模式。

  在 Android 6.0+ 中，当 AnyConnect 由于节电模式而转换为“已暂停”(Paused) 状态时，将出现一个弹出窗口，其中包含将 AnyConnect 加入节电模式白名单的选项。将 AnyConnect 加入白名单后，将允许继续使用节电模式，但不影响 AnyConnect 在后台运行的能力。

  当 AnyConnect 由于节电模式而暂停后，无论您是关闭节电模式还是将 AnyConnect 加入白名单，在这之后都必须手动重新连接，才能使 AnyConnect 脱离“已暂停”(Paused) 状态。

- 拆分 DNS 在任何 Android 4.4 设备上都无法运行，在 Samsung 5.x Android 设备上也无法运行。对于 Samsung 设备，唯一的解决方法是连接到禁用了拆分 DNS 的组。在其他设备上，必须升级到 Android 5.x 以接收此问题的修复。

  这是由 Android 4.4 中存在的一个已知问题（问题 #64819）导致的，该问题已在 Android 5.x 中修复，但未引入 Samsung 5.x android 设备中。

- 由于 Android 5.x 中的一个漏洞（Google 问题 #85758，思科问题 # CSCus38925），如果从“最近使用的应用”(recent apps) 屏幕中关闭 AnyConnect 应用，该应用可能无法正常运行。若要恢复正常运行，请在**设置 (Settings)** 中终止 AnyConnect，然后再重新启动。

- 在 Samsung 移动设备上，**设置 (Settings) > Wi-Fi > 智能网络交换机 (Smart network switch)** 允许从 WIFI 切换到 LTE（当 Wi-Fi 连接处于非最佳状态时），以保持稳定的 Internet 连接。这还会导致暂停并重新连接活动的 VPN 隧道。思科建议关闭此设置，因为它可能会导致不断地重新连接。

- 在支持多个活动用户的 Android 5.0 (Lollipop) 上，VPN 连接只能为一个用户通过隧道发送数据，而不能为设备上的所有用户都这样做。后台数据流可能会以明文形式传输。

- 由于 Android 4.3.1 中的一个漏洞（Google 问题 #62073），使用 AnyConnect ICS+ 软件包的用户无法输入非完全限定域名。例如，用户无法键入“internalhost”，他们必须键入“internalhost.company.com”。

- HTC One 上对 Android 4.3 的 AT&T 固件更新（软件版本：3.17.502.3）不支持“HTC AnyConnect”。客户必须卸载“HTC AnyConnect”，并安装“AnyConnect ICS+”。（HTC AnyConnect 将在国际版本上运行，软件版本为 3.22.1540.1）。请在**设置 (Settings) > 关于 (About) > 软件信息 (Software information) > 软件编号 (Software number)** 中检查设备上的软件版本。

- 非常值得高兴的是，Google 问题 #70916（如果管理员已将 Android 隧道的 MTU 设置为低于 1280，VPN 连接将失败）已在 Android 5.0 (Lollipop) 中得到解决。以下问题信息可供参考：

  由于 Android 4.4.3 中的一个回归问题（Google 问题 #70916，思科 CSCup24172），如果管理员已将 Android 隧道的 MTU 设置为低于 1280，VPN 连接将失败。已向 Google 报告此问题，需要使用新的操作系统版本才能纠正 Android 4.4.3 中引入的回归问题。若要解决此问题，请确保前端管理员未将隧道 MTU 配置为低于 1280。

  遇到此问题时，最终用户将看到以下消息：`无法应用系统配置设置。不会建立 VPN 连接 (System configuration settings could not be applied.A VPN connection will not be established)`，而且系统将报告 AnyConnect 调试日志：

```
E/vpnandroid( 2419): IPCInteractionThread: NCSS: General Exception occured, telling client
E/vpnandroid( 2419): java.lang.IllegalStateException: command '181 interface fwmark rule add tun0'
failed with '400 181 Failed to add fwmark rule (No such process)'
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1473)
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1419)
E/vpnandroid( 2419): at
com.cisco.android.nchs.aidl.IICSSupportService$Stub$Proxy.establish
(IICSSupportService.java:330)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.VpnBuilderWrapper.establish
(VpnBuilderWrapper.java:137)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.NCSSIPCServer.callServiceMethod
(NCSSIPCServer.java:233)
E/vpnandroid( 2419): at
com.cisco.android.nchs.ipc.IPCInteractionThread.handleClientInteraction
(IPCInteractionThread.java:230)
E/vpnandroid( 2419): at com.cisco.android.nchs.ipc.IPCInteractionThread.run
(IPCInteractionThread.java:90)
E/acvpnagent( 2450): Function: ApplyVpnConfiguration
File: NcssHelper.cpp Line: 740 failed to establish VPN
E/acvpnagent( 2450): Function: PluginResult AndroidSNAKSystem::configDeviceForICS()
File: AndroidSNAKSystem.cpp Line: 665 failed to apply vpn configuration
E/acvpnagent( 2450): Function: virtual PluginResult AndroidSNAKSystem::ApplyConfiguration()
File: AndroidSNAKSystem.cpp Line: 543 Failed to Configure System for VPN.
```

- 非常值得高兴的是，Android 4.4 (KitKat) 漏洞 Google 问题 #61948（AnyConnect 用户将在 VPN 连接期间遇到数据包丢失率过高的问题/用户将遇到超时问题）已在 Google Android 4.4.1 版本中得到解决，Google 已开始通过软件更新向部分设备分发该版本。以下问题信息可供参考：

  由于 Android 4.4 中的一个漏洞（问题 #61948，也可查看思科支持更新），AnyConnect 用户将在 VPN 连接期间遇到数据包丢失率过高的问题。在运行 Android 4.4 并使用 AnyConnect ICS+ 的 Google Nexus 5 上，已发现该漏洞。用户在尝试访问某些网络资源时，将遇到超时问题。此外，在 ASA 日志中，将显示一条系统日志消息，其中包含类似于“正在传输大数据包 1420（阈值 1405）”(Transmitting large packet 1420 [threshold 1405]) 的文本。

  在 Google 为 Android 4.4 提供修复之前，VPN 管理员可以通过配置以下 sysopt connection tcpmss <mss size>，暂时减小 ASA 上 TCP 连接的最大分段大小。此参数的默认值为 1380 字节。请将此值减去 ASA 日志中所示两个值之间的差值。在上述示例中，差值是 15 字节；因此，该值不应该超过 1365。减小此值会对已连接 VPN 并传输大数据包的用户带来性能上的负面影响。

- Android 版 AnyConnect 在使用称为 464xlat 的 IPv6 过渡机制连接到移动网络时，可能会遇到连接问题。已知受影响的设备包括连接到 T-Mobile 美国网络的 Samsung Galaxy Note III LTE。此设备默认为连接纯 IPv6 移动网络。尝试连接可能会导致移动连接中断，直到重启设备才恢复正常。

若要避免此问题，请使用 AnyConnect ICS+ 应用，并将设备设置更改为获取 IPv4 网络连接或使用 Wi-Fi 网络连接。对于连接到 T-Mobile 美国网络的 Samsung Galaxy Note III LTE，请按照 T-Mobile 提供的说明在设备上设置无线接入点名称 (APN)，并确保将 APN 协议设置为 IPv4。

- 当 VPN 中的专用 IP 地址范围与客户端设备外部接口的范围重叠时，AnyConnect ICS+ 软件包可能会出现问题。出现此路由重叠时，用户可能能够成功地连接到 VPN，但之后无法实际访问任何内容。已经在使用 NAT（网络地址转换）并分配 10.0.0.0 - 10.255.255.255 范围内地址的蜂窝网络上发现此问题，其原因是 AnyConnect 对 Android VPN Framework 中路由的控制能力有限。供应商特定 Android 软件包具有完整的路由控制能力，在这种情况下可能会表现得更好。
- 运行 Android 4.0 (ICS) 的华硕平板电脑可能缺少 TUN 驱动程序。这将导致 AVF AnyConnect 失败。
- 当 VPN 连接有效时，Android 安全规则会阻止设备发送和接收多媒体消息传送服务 (MMS) 消息。如果您尝试在 VPN 连接有效时发送 MMS 消息，大多数设备和服务提供商会显示一个通知。当 VPN 未连接时，Android 允许发送和接收消息。
- 由于 Google 问题 41037，从剪贴板粘贴文本时，会在文本前面插入一个空格。在 AnyConnect 中，复制一次性密码之类的文本时，用户必须删除这个错误的空格。

美洲总部
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

亚太区总部
Cisco Systems (USA) Pte. Ltd.
Singapore

欧洲总部
Cisco Systems International BV
Amsterdam, The Netherlands